PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 2, February 2012, Pages 513–518
S 0002-9939(2011)11236-X
Article electronically published on August 11, 2011

NON-CYCLIC ALGEBRAS WITH n-CENTRAL ELEMENTS

ELIYAH MATZRI, LOUIS H. ROWEN, AND UZI VISHNE

(Communicated by Harm Derksen)

Abstract. We construct, for any prime p, a non-cyclic central simple algebra of degree p^2 with p^2-central elements. This construction answers a problem of Peter Roquette.

1. Introduction

Let A be a division algebra, finite dimensional over the center F. An element $a \in A$ is called 'n-central' if $a^n \in F$ but $a^{n'} \notin F$ for every proper divisor n' of n.

The degree of the algebra is, by definition, the square root of its dimension over the center. The dimension of every maximal subfield is equal to the degree. The algebra is 'cyclic' if it has a maximal cyclic subfield. A cyclic algebra of degree n has n-cyclic elements by the Skolem-Noether theorem. When one attempts to show that an algebra is not cyclic, the best way is often to show that there are no n-cyclic elements. Therefore, it is natural to examine the converse and ask if the existence of n-cyclic elements in an algebra of degree n implies cyclicity.

Standard techniques reduce the problem to algebras of prime-power degree. Albert settled this problem for p-algebras, when he showed that an algebra of degree p^e in characteristic p is cyclic iff it has a p^e-central element [3, Theorem VII.26]. We therefore assume $\mathrm{char} F \neq p$.

When a is p^e-central and F contains primitive roots of unity of order p^e, $F[a]$ is a cyclic maximal subfield. In prime degree, even without roots of unity, Albert has shown that the existence of a p-central element implies cyclicity [3, Theorem XI.4]; his intricate construction can be explained in terms of the corestriction, [8], [7].

The problem remains when n is a non-prime prime power and F does not have roots of unity of order n. Albert himself provided a counterexample [1], namely a non-cyclic algebra of degree 4 that has 4-central elements. The odd-degree case remained open and became known as Roquette's problem.

In this paper we prove:

Theorem 1.1. *For any prime p there is a non-cyclic algebra of degree p^2, with a p^2-central element.*

The constructed example is a crossed product over a field F which has roots of unity of order p (but clearly, not p^2).

Received by the editors September 6, 2010 and, in revised form, December 5, 2010.
2010 *Mathematics Subject Classification.* Primary 16K20.

2. Abelian crossed products

A central simple algebra is a crossed product if it has a subfield Galois over the center. Such algebras, with abelian Galois groups, were first constructed by Dickson. They were studied by Amitsur-Saltman [4] and were used in following years to provide various counterexamples. Let us denote henceforth $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Our focus is in degree p^2, so let us summarize what we need from [4] regarding crossed products with respect to G:

Remark 2.1. Let K/F be a Galois extension of fields with Galois group

$$\mathrm{Gal}(K/F) = \langle \sigma_1, \sigma_2 \rangle \cong G,$$

and let $b_1, b_2, u \in K^\times$ be elements satisfying the equations

$$\begin{aligned} \sigma_i(b_i) &= b_i, \\ \sigma_2(b_1)b_1^{-1} &= \mathrm{N}_{\sigma_1}(u), \\ \sigma_1(b_2)b_2^{-1} &= \mathrm{N}_{\sigma_2}(u)^{-1}. \end{aligned} \tag{1}$$

Then the algebra $A = K[z_1, z_2]$, defined by the relations $z_i k z_i^{-1} = \sigma_i(k)$ for $k \in K$, $z_i^p = b_i$ and $z_2 z_1 = u z_1 z_2$, is a central simple algebra over F containing K as a maximal subfield, and every such algebra has this form.

The algebra defined above is denoted by $(K/F, \{\sigma_1, \sigma_2\}, \{b_1, b_2, u\})$.

Remark 2.2. The conditions (1) imply

$$\mathrm{N}_{K/F}(u) = 1, \tag{2}$$

and on the other hand, if (2) holds, then one can solve (1) with $b_1, b_2 \in K$, using Hilbert's theorem 90 for $\mathrm{N}_{\sigma_1}(u) \in K^{\sigma_1}$ and $\mathrm{N}_{\sigma_2}(u) \in K^{\sigma_2}$.

Let us assume that F has a pth root of unity, which we denote by ρ.

Remark 2.3. If we add the assumption

$$\mathrm{N}_{\sigma_1}(u) = \rho, \tag{3}$$

then z_1 becomes a p^2-central element. (Indeed, $z_1^{p^2} = b_1^p \in K^{\langle \sigma_1, \sigma_2 \rangle} = F$, whereas b_1 is not fixed by σ_2.) Moreover, (3) implies (2).

3. The example

Fix the prime number p. Let K/F be a Galois extension with Galois group $\mathrm{Gal}(K/F) = \langle \sigma_1, \sigma_2 \rangle \cong G$, where $\rho \in F$ is a pth root of unity, and let $b_1, b_2, u \in K^\times$ be elements satisfying the equations (1) and (3). Let

$$A = (K/F, \{\sigma_1, \sigma_2\}, \{b_1, b_2, u\})$$

be the corresponding crossed product (the existence of a division algebra of this form is proven below).

Let λ_1, λ_2 be indeterminates over F, and consider the subalgebra $A^\diamond$ of $A \otimes F(\lambda_1, \lambda_2)$, defined as follows. Let $F^\diamond = F(\lambda_1^p, \lambda_2^p)$ and $K^\diamond = K(\lambda_1^p, \lambda_2^p)$, with the action of σ_1, σ_2 extended to $K^\diamond$ by acting trivially on $F(\lambda_1, \lambda_2)$. The elements $b_1^\diamond = \lambda_1^p b_1$, $b_2^\diamond = \lambda_2^p b_2$ and $u^\diamond = u$ satisfy the identities (1) and (3). Letting $z_1^\diamond = \lambda_1 z_1$ and $z_2^\diamond = \lambda_2 z_2$, we have $z_i^{\diamond p} = b_i^\diamond$ and $z_2^\diamond z_1^\diamond = u^\diamond z_1^\diamond z_2^\diamond$, so $A^\diamond = K^\diamond[z_1^\diamond, z_2^\diamond]$ is the crossed product $(K^\diamond/F^\diamond, \{\sigma_1, \sigma_2\}, \{b_1^\diamond, b_2^\diamond, u^\diamond\})$.

Moreover, $b_1^{\diamond p} \in F^\diamond$, so $z_1^\diamond \in A^\diamond$ is a p^2-central element. Powers of λ_1 and λ_2 provide a $\mathbb{Z} \times \mathbb{Z}$-grading of $A_0^\diamond = K_0^\diamond[z_1^\diamond, z_2^\diamond]$, where $K_0^\diamond$ is the ring of polynomials $K[\lambda_1^p, \lambda_2^p]$. We order $\mathbb{Z} \times \mathbb{Z}$ lexicographically and denote by $\bar{f}$ the leading coefficient of $f \in A_0^\diamond$, namely when $f = \sum_{i,j} a_{ij} \lambda_1^i \lambda_2^j$ for $a_{ij} \in A$, $\bar{f}$ is the non-zero a_{ij} with largest (i, j).

Remark 3.1. If $f, g \in A_0^\diamond$ commute, then $\bar{f}, \bar{g}$ commute in A.

The grading of $A_0^\diamond$ should be contrasted with the G-grading of A via $A = \bigoplus K z_1^i z_2^j$, for which such a statement cannot possibly hold.

Lemma 3.2. *If $A^\diamond$ is cyclic, then A has a cyclic maximal subfield intersecting K non-trivially.*

Proof. Suppose $L^\diamond \subseteq A^\diamond$ is a cyclic extension of degree p^2 of $F^\diamond$, and let τ be a generator of $\mathrm{Gal}(L^\diamond/F^\diamond)$. By the above remark, the F-subalgebra of A, generated by the leading coefficients of elements in $L^\diamond$, is a subfield, which we denote L.

By Skolem-Noether, there is an element $w \in A_0^\diamond$, conjugation by which induces τ on $L^\diamond$. Clearly the ring of central quotients of $L^\diamond \cap A_0$ is $L^\diamond$, and if $f \in L^\diamond \cap A_0$, then $\bar{w}\bar{f} = \overline{\tau(f)}\bar{w}$; so conjugation by $\bar{w}$ preserves L. Since $L^\diamond / L^{\diamond \tau^p}$ is cyclic, there is an element $g \in L^\diamond \cap A_0^\diamond$ such that $\tau^p(g) = \rho g$; then $L^\diamond = F^\diamond[g]$. In particular $w^p g = \rho g w^p$, and so $\bar{w}^p \bar{g} = \rho \bar{g} \bar{w}^p$. Therefore, the order of the automorphism $\bar{\tau}$ induced by $\bar{w}$ on L is p^2, so L/F is a cyclic extension of degree p^2. Moreover since $\bar{\tau}^p(\bar{g}) = \rho \bar{g}$, we must have $L = F[\bar{g}]$.

For every element $f \in A_0^\diamond$, $\bar{f}$ has the form $a z_1^i z_2^j$ for $a \in K$, and clearly $\bar{f}^p \in K$. Since $\bar{g}^p \notin F$, L intersects K non-trivially, and in fact $L \cap K = F[\bar{g}^p]$. □

The reduction in Lemma 3.2 gains more power from the following observation: if L/F is a cyclic extension of degree p^2 (and $\rho \in F$), then ρ is a norm in the intermediate extension L'/F [2, Theorem IX.10].

Corollary 3.3. *Let K/F be a Galois extension with Galois group G. Suppose that ρ is a norm from K to an intermediate subfield, but not from an intermediate subfield to F.*

Then there is an algebra A, containing K as a maximal subfield, such that $A^\diamond$ is non-cyclic of degree p^2 and with a p^2-central element.

Proof. Choosing the generators properly, we assume that $\rho = \mathrm{N}_{\sigma_1}(u)$ for some $u \in K$, so let $b_1, b_2 \in K$ solve (1) as in Remark 2.2, and take A to be the corresponding crossed product, $(K/F, \{\sigma_1, \sigma_2\}, \{b_1, b_2, u\})$. Then $\lambda_1 z_1$ is p^2-central in $A^\diamond$ (as z_1 is p^2-central in A), but $A^\diamond$ is non-cyclic, for otherwise some intermediate subfield of K/F would be extendable to a cyclic subfield of dimension p^2 in A, which contradicts the no-norm assumption. □

Our goal, therefore, is to construct a Galois extension K/F with Galois group G, such that ρ is a norm in the extension K/K^{σ_1} but not in any of the intermediate extensions over F.

Lemma 3.4. *Let k be a field containing a pth root of unity ρ, but no roots of unity of order p^2. Let π be an indeterminate over k, and take $F = k(\pi^p)$ and $K = k(\pi)[t \mid t^p = \rho(1 - \pi^p)]$.*

Then K/F is a Galois extension with Galois group G, such that (for a suitable choice of σ_1) ρ is a norm in K/K^{σ_1}, but not in any intermediate extension over F.

Proof. The automorphism group acts via

$$\begin{aligned} \sigma_1 &: t \mapsto t, \quad \pi \mapsto \rho\pi, \\ \sigma_2 &: t \mapsto \rho t, \quad \pi \mapsto \pi; \end{aligned}$$

in particular, $\mathrm{N}_{\sigma_1}(1-\pi) = \prod_j (1-\rho^j\pi) = 1-\pi^p$, so $\mathrm{N}_{\sigma_1}(t(1-\pi)^{-1}) = \rho$. The intermediate subfields of $F \subset K$ are

$$K^{\sigma_2} = k(\pi),$$

and, for every $\ell = 0, \dots, p-1$,

$$K^{\sigma_1\sigma_2^{-\ell}} = k(\pi^p, \pi^\ell t).$$

It remains to show that ρ is not a norm from intermediate subfields to F. Since ρ is not a p-power in K, it suffices to verify that each intermediate subfield is totally ramified with respect to some valuation of F. Consider first the π-adic valuation: since K/F is ramified, $k(t)$ is the maximal unramified subfield, so every other subfield is totally ramified with respect to this valuation, and $k(t)$ itself is totally ramified over $F = k(t^p)$ with respect to the t-adic valuation. □

Notice that in this example, $u = t(1-\pi)^{-1}$ satisfies

$$\sigma_2(u) = \rho u. \tag{4}$$

In summary, let K/F be the extension given in Lemma 3.4 and let $u, b_1, b_2 \in K$ be elements satisfying (1), (3); e.g., taking

$$\begin{aligned} u &= t(1-\pi)^{-1}, \quad \text{and} \\ b_1 &= t, \end{aligned}$$

one can solve $\sigma_1(b_2)b_2^{-1} = \mathrm{N}_{\sigma_2}(u)^{-1}$ for $b_2 \in K^{\sigma_2}$, obtaining (up to scalars)

$$b_2 = \sum_{i=0}^{p-1} (-1)^{pi} \rho^i \prod_{j=0}^{i-1} \frac{(1-\pi^p)}{(1-\rho^j\pi)^p}.$$

Let $A = (K/F, \{\sigma_1, \sigma_2\}, \{b_1, b_2, u\})$. By Corollary 3.3, $A^\diamond$ has a p^2-central element but is not cyclic, as claimed in Theorem 1.1.

In particular, for $p = 2$, the center of $A^\diamond$ is a purely transcendental extension of degree 3 of k where $\sqrt{-1} \notin k$, precisely as in [1], where k is assumed to be 'a field of real numbers'.

4. The exponent of the counterexample

We conclude by showing that for p odd, the example constructed above has exponent p^2. We first consider a more general case.

Recall (again from [4]) the following facts about elementary abelian crossed products of degree p^2:

Remark 4.1. (a) If $u = 1$, then $A = (K/F, \{\sigma_1, \sigma_2\}, \{b_1, b_2, u\})$ decomposes as $K^{\sigma_1}[z_2] \otimes K^{\sigma_2}[z_1]$.

(b) For any $a_1, a_2 \in K$, the change of variables

$$z_1 \mapsto a_1 z_1, \qquad z_2 \mapsto a_2 z_2$$

induces an isomorphism from $(K/F, \{\sigma_1, \sigma_2\}, \{b_1, b_2, u\})$ to

$$(K/F, \{\sigma_1, \sigma_2\}, \{b_1', b_2', u'\}),$$

where

$$\begin{aligned} b_1' &= \mathrm{N}_{\sigma_1}(a_1)b_1, \\ b_2' &= \mathrm{N}_{\sigma_2}(a_2)b_2, \text{ and} \\ u' &= \sigma_2(a_1)a_1^{-1}a_2\sigma_1(a_2)^{-1}u. \end{aligned}$$

(c) $(K/F, \{\sigma_1, \sigma_2\}, \{b_1, b_2, u\})^{\otimes p} \sim (K/F, \{\sigma_1, \sigma_2\}, \{b_1^p, b_2^p, u^p\})$.

Lemma 4.2. *Suppose $p = 2$. Let $A = (K/F, \{\sigma_1, \sigma_2\}, \{b_1, b_2, u\})$ be a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$-crossed product for which the defining constants satisfy the conditions* (1), (3) *and* (4).

Then A decomposes as a product of quaternion algebras,

$$A \cong K^{\sigma_1}[z_1z_2] \otimes K^{\sigma_1\sigma_2}[(1-u^{-1})z_1].$$

Proof. Take $a_1 = b_1^{-1}$ and $a_2 = b_2^{-1}$ in Remark 4.1(b) to get

$$A^{\otimes 2} \sim (K/F, \{\sigma_1, \sigma_2\}, \{1, 1, 1\}) \sim F;$$

the fact that z_1z_2 and $(1-u^{-1})z_1$ commute readily gives the asserted decomposition. □

Lemma 4.3. *Assume p is odd. Let $A = (K/F, \{\sigma_1, \sigma_2\}, \{b_1, b_2, u\})$ be a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$-crossed product for which the defining constants satisfy the conditions* (1), (3) *and* (4). *Then*

(1) $A^{\otimes p} \sim (K^{\sigma_2}/F, \sigma_1, b_1^p)$, *and*
(2) $\exp(A)$ *divides p iff ρ is a norm in K^{σ_2}/F.*

Proof. From Equation (4) it follows that $\mathrm{N}_{\sigma_2}(u) = (-1)^{p-1}u^p$. Taking $a_1 = 1$ and $a_2 = b_2^{-1}$ presents the crossed product $(K/F, \{\sigma_1, \sigma_2\}, \{b_1^p, b_2^p, u^p\})$ as

$$A^{\otimes p} \sim (K/F, \{\sigma_1, \sigma_2\}, \{b_1^p, 1, 1\}),$$

which is a tensor product of the split algebra $(K^{\sigma_1}/F, \sigma_2, 1)$ and the cyclic algebra $(K^{\sigma_2}/F, \sigma_1, b_1^p)$. We note that in spite of the inherent asymmetry of conditions (3) and (4), the second component, and thus $A^{\otimes p}$ itself, corresponds to the cup product $(\alpha_1) \cup (\alpha_2) \in \mathrm{H}^2(F, \mu_p)$, where $(\alpha_i) \in \mathrm{H}^1(F, \mu_p)$ represents K^{σ_i}.

The exponent $\exp(A)$ divides p iff $(K^{\sigma_2}/F, \sigma_1, b_1^p)$ splits, which by Wedderburn's criterion is the case iff $b_1^p = \mathrm{N}_{\sigma_1}(b_1)$ is a norm in K^{σ_2}/F. But since $b_1^{-1}u \in K^{\sigma_2}$ by conditions (3) and (4), $\mathrm{N}_{\sigma_1}(b_1)$ is a norm iff $\rho = \mathrm{N}_{\sigma_1}(u)$ is.

In the case $p = 2$, take $a_1 = b_1^{-1}$ and $a_2 = b_2^{-1}$ to get

$$A^{\otimes 2} \sim (K/F, \{\sigma_1, \sigma_2\}, \{1, 1, 1\}) \sim F;$$

commutation of z_1z_2 with $(1-u^{-1})z_1$ readily demonstrates the given decomposition. □

Therefore, when $p = 2$ our example has exponent 2, but since we require ρ to not be a norm from subfields, every algebra constructed along the lines of our example for an odd p will have exponent p^2.

The non-cyclic algebra with 4-central elements constructed by Albert in 1938 has exponent 4. Apparently he was not satisfied and had a Ph.D. student publish in 1941 another example, this time with exponent 2 [5].

We thus pose the following problem:

Question 4.4. Let p be an odd prime. Is every central simple algebra of degree p^2 and exponent p that has a p^2-central element necessarily cyclic?

References

[1] A.A. Albert, *Non-cyclic algebras with pure maximal subfields*, Bull. AMS **44**, 576–579 (1938). MR1563796

[2] A.A. Albert, Modern Higher Algebra, University of Chicago Press, 1937.

[3] A.A. Albert, Structure of Algebras, Amer. Math. Soc. Coll. Publ. **XXIV**, AMS, 1961. MR0123587 (23:A912)

[4] S. Amitsur and D. Saltman, *Generic Abelian crossed products and p-algebras*, J. Algebra **51**(1), 76–87 (1978). MR0491789 (58:10988)

[5] R. Dubisch, *Non-cyclic algebras of degree four and exponent two with pure maximal subfields*, Bull. Amer. Math. Soc. **47**, 131–133 (1941). MR0003623 (2:246b)

[6] A. Auel, E. Brussel, S. Garibaldi and U. Vishne, *Open problems on central simple algebras*, Transformation Groups **16**(1), 219–264 (2011).

[7] J. Minác and A. Wadsworth, *Division algebras of prime degree and maximal Galois p-extensions*, Canad. J. Math. **59**(3), 658–672 (2007). MR2319163 (2008c:16029)

[8] U. Vishne, *Galois cohomology of fields without roots of unity*, J. Algebra **279**(2), 451–492 (2004). MR2078127 (2005e:12008)

Department of Mathematics, The Technion, Haifa 32000, Israel
E-mail address: elimatzri@gmail.com

Department of Mathematics, Bar-Ilan University, Ramat-Gan, 52900, Israel
E-mail address: rowen@math.biu.ac.il

Department of Mathematics, Bar-Ilan University, Ramat-Gan, 52900, Israel
E-mail address: vishne@math.biu.ac.il